

# Remarques sur le premier cas du théorème de Fermat sur les corps de nombres

Alain Kraus

**Abstract.** The first case of Fermat's Last Theorem for a prime exponent  $p$  can sometimes be proved using the existence of local obstructions. In 1823, Sophie Germain has obtained an important result in this direction by establishing that, if  $2p + 1$  is a prime number, the first case of Fermat's Last Theorem is true for  $p$ . In this paper, we investigate such obstructions over number fields. We obtain analogous results on Sophie Germain type criteria, for imaginary quadratic fields. Furthermore, extending a well known statement over  $\mathbb{Q}$ , we give an easily testable condition which allows occasionally to prove the first case of Fermat's Last Theorem over number fields for a prime number  $p \equiv 2 \pmod{3}$ .

**AMS Mathematics Subject Classification :** 11D41

**Keywords :** First Case of Fermat's Last Theorem - Number fields.

## INTRODUCTION

Soient  $K$  un corps de nombres et  $p$  un nombre premier impair. On dit que le premier cas du théorème de Fermat est vrai sur  $K$  pour l'exposant  $p$ , s'il n'existe pas d'éléments  $x, y, z$  dans l'anneau d'entiers  $O_K$  de  $K$  tels que

$$x^p + y^p + z^p = 0 \quad \text{et} \quad (xyz)O_K + pO_K = O_K.$$

En 1994, A. Wiles a démontré qu'il en est ainsi pour le corps  $\mathbb{Q}$ , indépendamment du fait que  $xyz$  soit premier avec  $p$  ([Wi]). En 2004, ce résultat a été étendu au corps  $\mathbb{Q}(\sqrt{2})$  par F. Jarvis et P. Meekin ([Ja-Me]). Récemment, N. Freitas et S. Siksek ont accompli des progrès importants concernant l'équation de Fermat sur les corps totalement réels ([Fr-Si]).

On s'intéresse dans cet article au premier cas du théorème de Fermat. Il est bien connu que la présence d'obstructions locales permet de le démontrer sur  $\mathbb{Q}$  pour certains exposants  $p$ . Historiquement, le premier résultat spectaculaire à ce sujet a été obtenu par S. Germain en 1823, qui a démontré que si  $2p + 1$  est un nombre premier, le premier cas du théorème de Fermat est vrai sur  $\mathbb{Q}$  pour l'exposant  $p$ . Cet énoncé a été généralisé par de nombreux mathématiciens, notamment par Wendt en 1884 qui a obtenu une généralisation en termes du résultant des polynômes de la forme  $X^n - 1$  et  $(X + 1)^n - 1$  (voir [Co-2] p. 430 et [Ri] p. 137). On se propose ici de démontrer un analogue du critère de Wendt dans le cas où  $K$  est un corps quadratique imaginaire.

Par ailleurs, si pour tout entier  $a$  compris entre 1 et  $\frac{p-3}{2}$ , on a

$$1 + a^p \not\equiv (1 + a)^p \pmod{p^2},$$

le premier cas du théorème de Fermat est vrai sur  $\mathbb{Q}$  pour l'exposant  $p$  ([Co-2] p. 430). Cette condition ne peut être satisfaite que si 3 ne divise pas  $p - 1$ . F.H. Hao et C.J. Parry ont étendu ce critère aux corps quadratiques dont l'anneau d'entiers possède un idéal premier au-dessus de  $p$  de degré résiduel 1 ([Ha-Pa]). On obtient ici une généralisation de cet énoncé à d'autres familles de corps de nombres. Pour tout nombre premier  $p \geq 5$  vérifiant cette condition modulo  $p^2$ , cela permet par exemple d'établir le premier cas du théorème de Fermat pour  $p$ , sur les corps cubiques purs, et sur des corps purs de degré sur  $\mathbb{Q}$  arbitrairement grand.

J'ai bénéficié de nombreuses remarques de D. Bernardi pendant la rédaction de cet article. Je l'en remercie vivement ici.

## I. Énoncé des résultats

Pour tout corps de nombres  $K$ , notons  $O_K$  son anneau d'entiers et  $h_K$  son nombre de classes. La lettre  $p$  désigne un nombre premier impair.

### 1. Le critère de Wendt sur les corps quadratiques imaginaires

Soit  $K$  un corps quadratique imaginaire. Pour tout entier  $n \geq 1$ , notons  $W_n$  le résultant des polynômes  $X^n - 1$  et  $(X + 1)^n - 1$ .

**Théorème 1.** *Supposons les conditions suivantes satisfaites :*

- 1) *on a  $h_K \not\equiv 0 \pmod{p}$ .*
- 2) *Il existe  $n \geq 1$  tel que  $q = np + 1$  soit un nombre premier décomposé dans  $K$  et que*

$$(n^n - 1)W_n \not\equiv 0 \pmod{q}.$$

*Alors, le premier cas du théorème de Fermat est vrai sur  $K$  pour l'exposant  $p$ .*

**Remarque 1.** Le nombre premier  $p$  étant donné, il n'existe qu'un nombre fini d'entiers  $n$  pour lesquels  $np + 1$  soit un nombre premier ne divisant pas  $W_n$ . Plus précisément, Dickson a démontré en 1909 que tout nombre premier de la forme  $np + 1$ , plus grand que  $(p-1)^2(p-2)^2 + 6p - 2$ , divise  $W_n$  ([Ri] p. 301). De plus,  $W_n = 0$  si 6 divise  $n$ . La question de savoir si pour tout  $p$ , il existe  $n$  tel que  $np + 1$  soit un nombre premier ne divisant pas  $W_n$  est toujours ouverte. Elle a été posée par Flye Sainte-Marie en 1880 et par Landau en 1913 (*loc. cit.*). Pour autant, on constate expérimentalement que la seconde condition du théorème est très souvent réalisée en pratique, excepté comme il se doit pour le corps  $\mathbb{Q}(\sqrt{-3})$  où elle ne l'est jamais si  $p \geq 5$ , à cause de la présence des racines cubiques de

l'unité. Si  $K$  n'est pas  $\mathbb{Q}(\sqrt{-3})$ , il est plausible qu'elle le soit toujours dès que  $p$  est plus grand qu'une constante ne dépendant que de  $K$ .

On déduit de l'égalité  $W_2 = -3$  un analogue du résultat de S. Germain sur  $K$ .

**Corollaire 1.** *Supposons  $h_K$  non divisible par  $p$  et que  $2p + 1$  soit un nombre premier décomposé dans  $K$ . Alors, le premier cas du théorème de Fermat est vrai sur  $K$  pour l'exposant  $p$ .*

**Corollaire 2.** *1) Si l'on a  $p \leq 10^6$ , le premier cas du théorème de Fermat est vrai sur le corps  $\mathbb{Q}(i)$  pour l'exposant  $p$ .*

*2) Si  $4p + 1$  ou  $8p + 1$  ou  $16p + 1$  est premier, le premier cas du théorème de Fermat est vrai sur  $\mathbb{Q}(i)$  pour l'exposant  $p$ .*

Démonstration : On a  $h_{\mathbb{Q}(i)} = 1$  et l'on peut vérifier la seconde condition du théorème pour  $p \leq 10^6$  à l'aide du logiciel de calculs Pari, environ en cinq minutes ([Pari]). Tout nombre premier congru à 1 modulo 4 est décomposé dans  $\mathbb{Q}(i)$ . Les factorisations de  $(n^n - 1)W_n$  pour  $n = 4, 8, 16$ , permettent alors d'établir la seconde assertion (cf. *loc. cit.*).

À titre indicatif, sur le corps  $\mathbb{Q}(i)$ , la liste des couples  $(p, n)$  pour  $p < 100$ , avec les plus petits entiers  $n$  pour lesquels le critère fonctionne est la suivante :

$(3, 4), (5, 8), (7, 4), (11, 8), (13, 4), (17, 8), (19, 40), (23, 20), (29, 8), (31, 76), (37, 4), (41, 20),$

$(43, 4), (47, 20), (53, 20), (59, 20), (61, 16), (67, 4), (71, 8), (73, 4), (79, 4),$

$(83, 32), (89, 44), (97, 4).$

## 2. Obstructions locales modulo $p^2$

**Théorème 2.** *Soient  $K$  un corps de nombres et  $p$  un nombre premier impair. Supposons les conditions suivantes satisfaites :*

*1) il existe un idéal premier de  $O_K$  au-dessus de  $p$ , de degré résiduel sur  $p$  égal à 1, et d'indice de ramification sur  $p$  inférieur ou égal à  $p - 1$ .*

*2) On a*

$$(1) \quad 1 + a^p \not\equiv (1 + a)^p \pmod{p^2} \quad \text{pour tout } a = 1, 2, \dots, \frac{p-3}{2}.$$

*Alors, le premier cas du théorème de Fermat est vrai sur  $K$  pour l'exposant  $p$ .*

**Remarque 2.** La condition (1) de l'énoncé ne peut être réalisée que si  $p = 3$  ou si  $p \equiv 2 \pmod{3}$ . En effet, si  $p \not\equiv 3$ , le polynôme  $(X + 1)^p - X^p - 1$  est divisible par

$p(X^2 + X + 1)$  et les racines cubiques de l'unité appartiennent à  $\mathbb{F}_p$  si  $p \equiv 1 \pmod{3}$ . L'ensemble des nombres premiers  $p < 150$  qui la vérifie est

$$\{3, 5, 11, 17, 23, 29, 41, 47, 53, 71, 89, 101, 107, 113, 131, 137, 149\}.$$

Expérimentalement, on constate qu'environ 84 pour cent des nombres premiers congrus à 2 modulo 3 satisfont la condition (1). Par exemple, il y a 39265 nombres premiers impairs, congrus à 2 modulo 3, plus petits que  $10^6$ , et 33316 d'entre eux passent positivement le test ; il y en a 30870 qui sont irréguliers et 13192 d'entre eux satisfont la condition (1).

**Corollaire 3.** *Soit  $p$  un nombre premier  $\geq 5$  vérifiant la condition (1). Soit  $d$  un entier rationnel distinct de  $\pm 1$ . Supposons que l'on soit dans l'un des cas suivants :*

- 1)  $K = \mathbb{Q}(\sqrt[3]{d})$  où  $d$  est sans facteurs cubiques,
- 2)  $K = \mathbb{Q}(\sqrt[n]{d})$  où  $p$  ne divise pas  $dn$ ,  $d$  est sans facteurs carrés et  $n \equiv 1 \pmod{p-1}$ ,
- 3)  $K$  est une extension de  $\mathbb{Q}$ , totalement ramifiée en  $p$ , dont le degré sur  $\mathbb{Q}$  est inférieur ou égal à  $p-1$ .

Alors, le premier cas du théorème de Fermat est vrai sur  $K$  pour l'exposant  $p$ .

**Remarque 3.** Dans l'énoncé de la seconde assertion, l'hypothèse selon laquelle  $d$  est distinct de  $\pm 1$  et sans facteurs carrés, sert à garantir que le polynôme  $X^n - d$  est irréductible sur  $\mathbb{Q}$ . Par ailleurs, si l'on spécifie  $d$  et  $p$ , on peut obtenir un énoncé plus précis. À titre indicatif, si  $n$  est un entier impair non multiple de 5, le premier cas du théorème de Fermat est vrai sur le corps  $\mathbb{Q}(\sqrt[n]{3})$ , pour l'exposant  $p = 5$ .

## II. Démonstration du théorème 1

Soit  $(x, y, z)$  un triplet d'éléments de  $O_K$  tel que

$$x^p + y^p + z^p = 0 \quad \text{et} \quad (xyz)O_K + pO_K = O_K.$$

Posons

$$D = xO_K + yO_K.$$

On a les égalités

$$(2) \quad D = xO_K + zO_K = yO_K + zO_K.$$

### 1. Lemmes préliminaires

Les égalités (2) et le lemme qui suit n'utilisent pas le fait que  $K$  est un corps quadratique imaginaire.

**Lemme 1.** *L'idéal*

$$\frac{(x+y)O_K}{D}$$

*est la puissance  $p$ -ième d'un idéal de  $O_K$ .*

Démonstration : On a l'égalité

$$(x+y)s = -z^p \quad \text{où} \quad s = \sum_{k=0}^{p-1} x^{p-1-k}(-y)^k.$$

Parce que  $x$  et  $y$  sont dans  $D$ , l'idéal  $D^{p-1}$  divise  $sO_K$ . On obtient l'égalité d'idéaux de  $O_K$

$$\left( \frac{(x+y)O_K}{D} \right) \left( \frac{sO_K}{D^{p-1}} \right) = \left( \frac{zO_K}{D} \right)^p.$$

Il suffit ainsi d'établir que l'on a

$$\frac{(x+y)O_K}{D} + \frac{sO_K}{D^{p-1}} = O_K.$$

Soit  $\mathfrak{q}$  un idéal premier non nul de  $O_K$  divisant  $\frac{(x+y)O_K}{D}$ . Il s'agit de montrer que  $\mathfrak{q}$  ne divise pas  $\frac{sO_K}{D^{p-1}}$ . Pour cela, on vérifie par récurrence que pour tout  $k \geq 1$ , on a

$$(-y)^k \equiv x^k \pmod{\mathfrak{q}D^k}.$$

Pour tout  $k$  compris entre 0 et  $p-1$ , on a donc

$$x^{p-1-k}(-y)^k \equiv x^{p-1} \pmod{\mathfrak{q}D^{p-1}},$$

d'où la congruence

$$s \equiv px^{p-1} \pmod{\mathfrak{q}D^{p-1}}.$$

Supposons que  $\mathfrak{q}$  divise  $\frac{sO_K}{D^{p-1}}$ . L'idéal  $\mathfrak{q}D^{p-1}$  divise alors  $(px^{p-1})O_K$ . Par ailleurs, l'égalité  $(xyz)O_K + pO_K = O_K$  entraîne que  $\mathfrak{q}D^{p-1}$  est premier avec  $pO_K$ , donc  $\mathfrak{q}D^{p-1}$  divise  $x^{p-1}O_K$ . On en déduit que  $\mathfrak{q}$  divise  $\frac{xO_K}{D}$ , puis que  $x$  est dans  $\mathfrak{q}D$ . L'élément  $x+y$  étant aussi dans  $\mathfrak{q}D$ , il en est de même de  $y$ . Cela contredit le fait que  $D$  est le plus grand commun diviseur de  $xO_K$  et  $yO_K$ , d'où le lemme.

Le fait que  $K$  soit un corps quadratique imaginaire intervient désormais de façon essentielle. On supposera de plus, ce qui n'est pas restrictif,

$$K \neq \mathbb{Q}(\sqrt{-3}).$$

En effet, on a  $h_{\mathbb{Q}(\sqrt{-3})} = 1$ , la seconde condition du théorème 1 est satisfaite pour  $p = 3$  (avec  $n = 2$ ) et ne l'est pas si  $p \geq 5$ . Par ailleurs, il est connu que le premier cas du

théorème de Fermat est vrai sur  $\mathbb{Q}(\sqrt{-3})$  pour l'exposant  $p = 3$ . Le théorème 1 est donc vrai pour le corps  $\mathbb{Q}(\sqrt{-3})$ .

Par hypothèse,  $p$  ne divise pas  $h_K$ . Il existe donc  $t \in \mathbb{N}$  tel que  $p$  divise  $th_K + 1$ . L'idéal  $D^{h_K}$  est principal. En particulier, il existe  $d \in O_K$  tel que l'on ait

$$(3) \quad D^{h_K t} = dO_K.$$

**Lemme 2.** *Il existe des éléments non nuls  $a, b, c$  dans  $O_K$  tels que l'on ait*

$$d(x + y) = a^p, \quad d(x + z) = b^p, \quad d(y + z) = c^p.$$

Démonstration : D'après le lemme 1, il existe un idéal  $I$  de  $O_K$  tel que l'on ait l'égalité  $(x + y)O_K = DI^p$ . On a donc

$$\left(D^{\frac{h_K t + 1}{p}} I\right)^p = d(x + y)O_K.$$

Parce que  $p$  ne divise pas  $h_K$ , l'idéal  $D^{\frac{h_K t + 1}{p}} I$  est principal. Le corps  $K$  étant quadratique imaginaire, distinct de  $\mathbb{Q}(\sqrt{-3})$ , les unités de  $O_K$  sont des puissances  $p$ -ièmes dans  $O_K$  (y compris si  $p = 3$ ), d'où l'existence d'un élément  $a \in O_K$  tel que  $d(x + y) = a^p$ . Les égalités (2) et (3) entraînent alors le résultat.

Soit  $n \geq 1$  un entier tel que  $q = np + 1$  soit un nombre premier vérifiant la seconde condition de l'énoncé du théorème.

**Lemme 3.** *Chaque idéal premier de  $O_K$  au-dessus de  $q$  divise  $(xyz)O_K$ .*

Démonstration: Supposons qu'il existe un idéal premier  $\mathfrak{q}$  de  $O_K$  au-dessus de  $q$  ne divisant pas  $(xyz)O_K$ . Il existe alors  $u \in O_K$  tel que l'on ait

$$u \equiv \left(\frac{x}{z}\right)^{\frac{q-1}{n}} \pmod{\mathfrak{q}}.$$

Le corps  $O_K/\mathfrak{q}$  est de cardinal  $q$ , d'où la congruence

$$u^n = 1 \pmod{\mathfrak{q}}.$$

L'égalité  $x^p + y^p + z^p = 0$  implique

$$u + 1 \equiv -\left(\frac{y}{z}\right)^{\frac{q-1}{n}} \pmod{\mathfrak{q}}.$$

On obtient ( $n$  est pair)

$$(u + 1)^n \equiv 1 \pmod{\mathfrak{q}},$$

ce qui entraîne que  $q$  divise  $W_n$ , d'où une contradiction et le résultat.

## 2. Fin de la démonstration du théorème 1

Quitte à diviser l'égalité  $x^p + y^p + z^p = 0$  par une puissance convenable de  $q$ , on peut supposer que  $(x, y, z)$  n'est pas nul modulo  $qO_K$ . Il existe donc un idéal premier  $\mathfrak{q}$  de  $O_K$  au-dessus de  $q$  tel que  $(x, y, z)$  soit non nul modulo  $\mathfrak{q}$ . Notons  $v_{\mathfrak{q}}$  la valuation sur  $K$  qui lui est associée. D'après le lemme 3, on peut supposer que l'on a

$$v_{\mathfrak{q}}(z) \geq 1,$$

auquel cas on a

$$v_{\mathfrak{q}}(x) = v_{\mathfrak{q}}(y) = 0.$$

En particulier,  $\mathfrak{q}$  ne divise pas  $D$  et d'après l'égalité (3), on a

$$v_{\mathfrak{q}}(d) = 0.$$

Par suite, on a  $v_{\mathfrak{q}}(d(y+z)) = 0$  et d'après le lemme 2 on obtient

$$v_{\mathfrak{q}}(c) = 0.$$

Pour la même raison, on a

$$v_{\mathfrak{q}}(b) = 0.$$

L'égalité  $2dz = b^p + c^p - a^p$  (lemme 2) et l'hypothèse selon laquelle  $q$  ne divise pas  $W_n$ , impliquent alors (comme dans la démonstration du lemme 3)

$$v_{\mathfrak{q}}(a) \geq 1.$$

Il en résulte que l'on a

$$v_{\mathfrak{q}}(x+y) \geq 1.$$

On a ainsi l'égalité

$$d(-z^p) = a^p s \quad \text{avec} \quad s = \sum_{k=0}^{p-1} x^{p-1-k} (-y)^k,$$

et la congruence

$$s \equiv px^{p-1} \pmod{\mathfrak{q}}.$$

On en déduit que  $v_{\mathfrak{q}}(s) = 0$ , donc  $\frac{z}{a}$  est une unité modulo  $\mathfrak{q}$ . On a  $dx \equiv b^p \pmod{\mathfrak{q}}$ , d'où

$$p \equiv \frac{s}{x^{p-1}} \equiv \left( \frac{-bz}{xa} \right)^p \pmod{\mathfrak{q}}.$$

Le corps  $O_K/\mathfrak{q}$  est de cardinal  $q$  et on a  $np = q - 1$ , d'où  $p^n \equiv 1 \pmod{\mathfrak{q}}$ , puis

$$p^n \equiv 1 \pmod{q}.$$

Puisque  $n$  est pair, on obtient

$$1 = (-1)^n = (np - q)^n \equiv n^n p^n \equiv n^n \pmod{q},$$

ce qui conduit à une contradiction, d'où le théorème.

### III. Démonstration du théorème 2

Elle est analogue à celle du théorème 1 de [Ha-Pa]. Soit  $\mathfrak{p}$  un idéal premier de  $O_K$  au-dessus de  $p$  de degré résiduel 1. Notons  $v_{\mathfrak{p}}$  la valuation sur  $K$  qui lui est associée. Posons  $e = v_{\mathfrak{p}}(p)$  l'indice de ramification de  $\mathfrak{p}$  sur  $p$ . Supposons qu'il existe  $x, y, z$  dans  $O_K$  tels que l'on ait

$$x^p + y^p + z^p = 0 \quad \text{et} \quad v_{\mathfrak{p}}(xyz) = 0.$$

Les corps  $O_K/\mathfrak{p}$  et  $\mathbb{F}_p$  étant isomorphes, il existe  $x_0, y_0, z_0 \in \mathbb{Z}$  non divisibles par  $p$  tels que

$$x \equiv x_0 \pmod{\mathfrak{p}}, \quad y \equiv y_0 \pmod{\mathfrak{p}}, \quad z \equiv z_0 \pmod{\mathfrak{p}}.$$

Il en résulte que l'on a

$$v_{\mathfrak{p}}(x^p - x_0^p) \geq \inf(e + 1, p) = e + 1,$$

d'où la congruence

$$x_0^p + y_0^p + z_0^p \equiv 0 \pmod{\mathfrak{p}^{e+1}}.$$

On en déduit que l'on a

$$x_0^p + y_0^p + z_0^p \equiv 0 \pmod{p^2}.$$

En particulier, on a

$$x_0 + y_0 + z_0 \equiv 0 \pmod{p},$$

d'où

$$(x_0 + y_0)^p + z_0^p \equiv 0 \pmod{p^2},$$

puis

$$(x_0 + y_0)^p \equiv x_0^p + y_0^p \pmod{p^2}.$$

On obtient

$$(4) \quad 1 + a^p \equiv (1 + a)^p \pmod{p^2} \quad \text{avec} \quad a \equiv x_0^{-1}y_0 \pmod{p^2}.$$

On a  $a \not\equiv 0 \pmod{p}$  et  $a \not\equiv -1 \pmod{p}$  car  $p$  ne divise pas  $z_0$ . Parce que (4) ne dépend que de la congruence de  $a$  modulo  $p$ , on peut supposer que l'on a  $1 \leq a \leq p - 2$ . Si  $a = \frac{p-1}{2}$ , alors  $a = 1$  est aussi solution de (4). Si l'on a  $\frac{p-1}{2} < a \leq p - 2$ , alors  $p - 1 - a$  satisfait (4) et  $1 \leq p - 1 - a \leq \frac{p-3}{2}$ . Cela contredit la condition (1), d'où le résultat.



## IV. Démonstration du corollaire 3

1) On a  $p \equiv 2 \pmod{3}$  car  $p$  satisfait la condition (1). Dans l'anneau d'entiers de  $\mathbb{Q}(\sqrt[3]{d})$ , il existe donc un idéal premier au-dessus de  $p$  de degré résiduel 1 ([Co-1], cor. 6.4.15 et th. 6.4.16), d'où la première assertion.

2) Posons  $K = \mathbb{Q}(\sqrt[n]{d})$ . Le polynôme  $X^n - d$  est irréductible sur  $\mathbb{Q}$ , de discriminant

$$(-1)^{\frac{n(n-1)}{2}} n^n d^{n-1}.$$

La congruence  $n \equiv 1 \pmod{p-1}$  implique  $d^n \equiv d \pmod{p}$ . Le fait que  $p$  ne divise pas  $dn$  entraîne alors l'existence d'un idéal premier de  $O_K$  au-dessus de  $p$  non ramifié de degré résiduel 1 ([Co-1], th. 4.8.13), d'où le résultat.

3) La dernière assertion est une conséquence directe du théorème 2.

## Bibliographie

- [Co-1] H. Cohen, A course in Computational Algebraic Number Theory, Springer-Verlag GTM **138**, 1993.
- [Co-2] H. Cohen, Number Theory Volume I : Tools and Diophantine Equations, Springer-Verlag GTM **239**, 2007.
- [Fr-Si] N. Freitas et S. Siksek, Modularity and the Fermat equation over totally real number fields, arXiv : 1307.3162v2 (2014), 32 pages.
- [Ha-Pa] F. H. Hao, C. J. Parry, The Fermat equation over quadratic fields, *J. Number Theory* **19** (1984), 115-130.
- [Ja-Me] F. Jarvis et P. Meekin, The Fermat equation over  $\mathbb{Q}(\sqrt{2})$ , *J. Number Theory* **109** (2004), 182-196.
- [Pari] C. Batut, D. Bernardi, K. Belabas, H. Cohen et M. Olivier, PARI-GP, version 2.3.3, Université de Bordeaux I, (2008).
- [Ri] P. Ribenboim, Fermat's Last Theorem for Amateurs, Springer-Verlag, 1999.
- [Wi] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math.* **141** (1995), 443-551.

2 avril 2014

Alain Kraus  
Université de Paris VI,  
Institut de Mathématiques,  
4 Place Jussieu, 75005 Paris,  
France  
e-mail : alain.kraus@imj-prg.fr